

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-252320

(43)Date of publication of application : 22.09.1997

(51)Int.Cl.

H04L 12/56

G06F 13/00

H04B 7/00

H04B 7/26

H04H 1/00

H04H 1/08

(21)Application number : 08-059745

(71)Applicant : SONY CORP

(22)Date of filing : 15.03.1996

(72)Inventor : ISHII MAKOTO

(54) DATA TRANSMITTER AND ITS METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To conduct digital data transmission adopting the high quality radio system for only specific users.

SOLUTION: An internet protocol(IP) packet 32 generated by an IP packet generating section 3 is ciphered by a ciphering section 33 and a medium access control(MAC) frame generating section 36 provides a MAC header to the ciphered packet and generates a MAC frame 37. Then a cyclic redundancy check(CRC) calculation section 38 generates a CRC code and adds it to the MAC frame 37 to generate a MAC frame 39. Then a section generating section 40 generates a section 41 of a moving picture experts group(MPEG)2 and divides it into transport packets 43 and sends the result from a server to a client via a communication satellite.

<hr size=2 width="100%" align=center>

CLAIMS

[Claim(s)]

[Claim 1] In data transmission equipment which performs data communications between a server and a client via a network, data can be transmitted to a client with radio system from a server via the 1st data communication channel in which bidirectional data communications are possible between client and said server. Compared with said 1st data communication channel, transmission capacity has the 2nd big data communication channel, and it said server. Data transmission equipment which transmits data according to a demand from said client to said client via said 2nd data communication channel based on Internet Protocol for transmitting and receiving digital data via a network between two or more systems.

[Claim 2] Said 1st data communication channel is a course which used a terrestrial communication network.

The data transmission equipment according to claim 1 which is the course for which said 2nd data communication channel used a communications satellite.

[Claim 3] The data transmission equipment according to claim 1 in which said Internet Protocol is a TCP/IP protocol.

[Claim 4] The data transmission equipment according to claim 3 which said server changes data to transmit into an IP packet and transmits this IP packet to said client via said 2nd communication path.

[Claim 5] The data transmission equipment according to claim 4 which said server generates a MAC frame by media access control (MAC) from said IP packet and transmits this MAC frame to said client via said 2nd communication path.

[Claim 6] The data transmission equipment according to claim 5 which said server enciphers said IP packet and generates said one MAC frame about said one enciphered IP packet.

[Claim 7] An IP address of a client which should receive data in a header of said MAC frame. A control bit for distinguishing whether data is media data according to a demand from a client or it is the control data for system management from a control bit which shows existence of a data encryption. The data transmission equipment according to claim 5 with which a bit which shows attached data length at the time of normalizing data length which is needed for enciphering data is contained.

[Claim 8] A means to encipher an IP packet which distributes said server to said client which advanced a demand by a peculiar encryption algorithm which only server concerned and the client concerned get to know. A means to create a MAC frame from said enciphered IP packet using media access control. A means to change into a section into which said MAC frame was specified by MPEG 2. The data transmission equipment according to claim 4 which has a means to change said section into a transport stream to which it was specified by MPEG 2 and a means to transmit said transport stream to said client via said 2nd communication path.

[Claim 9] The data transmission equipment according to claim 5 in which said server

and said client have further a means to inspect all the data bytes of said MAC framewith a CRC method.

[Claim 10]The data transmission equipment according to claim 5 which has further a means by which said server adds a CRC inspection bit about a MAC frame to the last of a MAC frame.

[Claim 11]The data transmission equipment according to claim 9 which has further a means by which said server adds a CRC inspection bit about a MAC frame to the last of a MAC frame.

[Claim 12]In a data distribution device which performs data communications between Kula and Yingde via a networkData can be transmitted to a client with radio system from the 1st interface connected with the data distribution device concerned at the 1st data communication channel in which bidirectional data communications are possible between clientsand the data distribution device concernedIt has the 2nd interface connected to the 2nd data communication channel with big transmission capacity compared with said 1st data communication channelA data distribution device which transmits data according to a demand from said client to said client via said 2nd data communication channel based on Internet Protocol for transmitting and receiving digital data via a network between two or more systems.

[Claim 13]The data distribution device according to claim 12 which changes data to transmit into an IP packet and transmits this IP packet to said client via said 2nd communication path.

[Claim 14]The data distribution device according to claim 13 which enciphers said IP packetgenerates a MAC frame by said one media access controland transmits the MAC frame concerned about said one enciphered IP packet.

[Claim 15]A means to encipher an IP packet distributed to said client which advanced a demand by a peculiar encryption algorithm which only data distribution device concerned and the client concerned get to knowA means to create a MAC frame from said enciphered IP packet using media access controlA means to change into a section into which said MAC frame was specified by MPEG 2The data distribution device according to claim 14 which has a means to change said section into a transport stream to which it was specified by MPEG 2and a means to transmit said transport stream to said client via said 2nd communication path.

[Claim 16]In a data receiver which performs data communications between servers via a networkData can be transmitted to the data receiver concerned with radio system from the 1st interface connected to the 1st data communication channel in which bidirectional data communications are possible between said server and the data receiver concernedand said serverIt has the 2nd interface connected to the 2nd data communication channel with big transmission capacity compared with said 1st data communication channelA data receiver which receives data from said server via said 2nd data communication channel based on Internet Protocol for transmitting and receiving digital data via a network between two or more systems.

[Claim 17]The data receiver according to claim 16 in which said data to receive is data of IP packet form.

[Claim 18]The data receiver according to claim 17 which incorporates a required IP packet selectively based on a header of a MAC frame by media access control contained in said data to receive.

[Claim 19]Are a data transmission method characterized by comprising the following which performs data communications between a server and a client via a network and said serverA data transmission method which transmits data according to a demand from said client to said client via said 2nd data communication channel based on Internet Protocol for transmitting and receiving digital data via a network between two or more systems.

The 1st data communication channel in which bidirectional data communications are possible between a server and a client.

The 2nd data communication channel with big transmission capacity compared with said 1st data communication channel that can transmit data to a client with radio system from said server.

[Claim 20]The data transmission method according to claim 19 which said 1st data communication channel is a course which used a terrestrial communication network and is the course for which said 2nd data communication channel used a communications satellite.

[Claim 21]The data transmission method according to claim 19 in which said Internet Protocol is a TCP/IP protocol.

[Claim 22]The data transmission method according to claim 21 which said server changes data to transmit into an IP packet and transmits this IP packet to said client via said 2nd communication path.

[Claim 23]The data transmission method according to claim 22 which said server generates a MAC frame by media access control (MAC) from said IP packet and transmits this MAC frame to said client via said 2nd communication path.

[Claim 24]The data transmission method according to claim 23 which said server enciphers said IP packet and generates said one MAC frame about said one enciphered IP packet.

[Claim 25]An IP address of a client which should receive data in a header of said MAC frameA control bit for distinguishing whether data is media data according to a demand from a client or it is the control data for system management from a control bit which shows existence of a data encryptionThe data transmission method according to claim 23 with which a bit which shows attached data length at the time of normalizing data length which is needed for enciphering data is contained.

[Claim 26]The data transmission method comprising according to claim 22:

A means to encipher an IP packet which distributes said server to said client which advanced a demand by a peculiar encryption algorithm which only server concerned

and the client concerned get to know.

A means to create a MAC frame from said enciphered IP packet using media access control.

A means to change into a section into which said MAC frame was specified by MPEG 2.

A means to change said section into a transport stream to which it was specified by MPEG 2 and a means to transmit said transport stream to said client via said 2nd communication path.

[Claim 27]The data transmission method according to claim 23 in which said server and said client have further a means to inspect all the data bytes of said MAC framewith a CRC method.

[Claim 28]The data transmission method according to claim 23 which has further a means by which said server adds a CRC inspection bit about a MAC frame to the last of a MAC frame.

[Claim 29]The data transmission method according to claim 27 which has further a means by which said server adds a CRC inspection bit about a MAC frame to the last of a MAC frame.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to data transmission equipment for offering multimedia data distribution serviceand a method for the samefor example using a communications satellite.

[0002]

[Description of the Prior Art]Conventionallyin the data distribution service using communications satellitessuch as television broadcastingdata flow was only one way from a data distribution person to a user. In recent yearsit came to be transmitted by transmission of the digital data using a communications satellite having been attained using the communications satellite also about the textand the digital image and voice data which are used not only by analog video and voice datasuch as television and a moviebut by computer etc. Herethe conventional data distribution service using communications satellitessuch as television broadcastingis a gestalt as for which many users use the data which the data distribution person distributed receiving simultaneously. On the other handwhen distributing the digital data used by computer etc. via a communications satellitethe function which distributes data to the specific user of the singular number or plurality from a data distribution person is called for.

[0003]

[Problem(s) to be Solved by the Invention] However in the conventional transmission system using a communications satellite since it being distribution of analog data and data distribution are only one way from a data distribution person to a user a check function is not provided with the error on transmission but there is a problem that the reliability of data communications is low. In distribution of digital data if at least 1 bit of errors arise to data by transmission the received data will become meaningless. In order to distribute such digital computer data with high quality with radio system it is necessary to secure the channel not only from a user to the data distribution of one way from a data distribution person to a user but a data distribution person but and in the conventional transmission system it does not have such a function.

[0004] In the conventional simultaneous transmissive communication or broadcasting system from a data distribution person to many users All Users receives the always same information use or an inspection is carried out and since there is no identification information of a system user individual there is a problem that distribution of data only to a specific user from a data distribution person cannot be performed.

[0005] It aims at providing data transmission equipment which can transmit digital data with radio system and a method for the same without making this invention in view of the problem of the conventional technology mentioned above and generating the error on transmission. An object of this invention is to provide data transmission equipment which can transmit digital data only to a specific client with radio system and a method for the same.

[0006]

[Means for Solving the Problem] In order to attain the purpose mentioned above data transmission equipment of this invention Data can be transmitted to a client with radio system from a server the 1st data communication channel in which bidirectional data communications are possible between clients and said server Compared with said 1st data communication channel transmission capacity has the 2nd big data communication channel and it said server Based on Internet Protocol for transmitting and receiving digital data via a network between two or more systems data according to a demand from said client is transmitted to said client via said 2nd data communication channel.

[0007] The data transmission method of this invention can transmit data to a client with radio system from a server the 1st data communication channel in which bidirectional data communications are possible between clients and said server It is a data transmission method which performs data communications between a server and a client via a network which has the 2nd data communication channel with big transmission capacity compared with said 1st data communication channel Said server transmits data according to a demand from said client to said client via said 2nd data communication channel based on Internet Protocol for transmitting and receiving digital data via a network between two or more systems.

[0008] In data transmission equipment of this invention and a method for the same. For

example in [if a client performs a predetermined request to a server via the 1st data communication channel] a server data according to the request concerned is changed based on Internet Protocol and this changed digital data is transmitted to a client via the 2nd data communication channel.

[0009] According to data transmission equipment by this invention and a method for the same transmission becomes possible from a server with high quality about large scale digital data at a client and transmission of digital data is further attained from a server only at a specific user.

[0010]

[Embodiment of the Invention] Data transmission equipment (information service system) concerning the embodiment of this invention and a method for the same are explained. The outline of the data transmission equipment for realizing data service which distributes the digital data (an image, sound, text, etc.) of multimedia is shown in drawing 1. In the data transmission equipment shown in drawing 1 the data donor A owns the data distribution device 4 as a server and the user B owns the data receiver 5 as a client. The data distribution device 4 and the data receiver 5 can communicate mutually via ISDN3 in which bidirectional communication is possible. Mass communication is possible at radio system via the communications satellite 2 to the data receiver 5 from the data distribution device 4.

[0011] The data flow in the data transmission equipment shown in drawing 1 is explained. It is assumed that the user B has signed the contract of delivery of multimedia data with the user donor A beforehand. Under the present circumstances it is assumed that the user's B data receiver 5 is equipped with the function in which data is receivable from the data donor's A data distribution device 4. The data donor A knows that the contract with the user B is made beforehand.

[0012] First the user B sends the request 6 of the purport that he would like to receive the predetermined service which the data donor A provides to the data donor A for example via ISDN3 as a terrestrial communication network. The method in particular of sending this REQUEST 6 may not be limited but may be decided by the kind of data or a contract state with a user for example mail, etc., may be sufficient as it. In accordance with a contract the data donor A may provide service beforehand without sending the request 6.

[0013] The request 6 from the user B sent to the data distribution device 4 is received by the data request reception part 7 and is sent to the data management part 9. The data management part 9 will perform the read request 10 of data to the data storing section 11 if the contract information and the request 6 of the user B check that it is that meaningful and it is satisfactory. The data storing section 11 sends the multimedia data 12 to the data creation part 13 having corresponded to the data read demand 10. In the data creation part 13 to the multimedia data 12 from the data storing section 11 IP-packet-izing, Encryption and MAC (Media Access Control) which were beforehand decided peculiar to the user B, Format conversion of the data

of frame-izingtransport-izing of MPEG(Moving Picutre Experts Group) 2etc. is performed. It mentions later about this data format conversion.

[0014]The multimedia data 12 from the data storing section 11 is sent to the communications satellite 2 by the data creation part 13 as the data 14creation or after format conversion is carried out. The data 14 sent via the communications satellite 2 can be received by all the users who are in the situation where not only the user's B data receiver 5 but data is receivable. The data receiver 5 receives all the data from the communications satellite 2and sorts out and receives the data according to the request 6 which he advanced from the inside.

[0015]That isthe data receiver 5 receives the data 14 of a large number containing the transmitted data according to the request 6 by the data receiving section 16. The data receiver 5 sorts out the data addressed to itselfthe data which he should receiveand the data (this is based also on a contract) which he can receive from the inside. This sorting is performed in the data selection part 18 of the data receiver 5. The data receiver 5 which the user B has is beforehand determined by the contract of the user B and the data donor A. Thereforethe characteristic data of other addressing to a user cannot be sorted out using the data receiver 5 which the user B has.

[0016]In the data selection part 18the data 19 in which what the user B receives is possible is altogether sent to the data decomposition part 20. The data addressed to user B sent to the data decomposition part 20 is disassembled or decodedturns into the multimedia data 21and is sent to the data execution part 22. By thisthe user B can receive the data addressed to user B which the user B requestedand this data service is completed. It may be continued over the case where reception of the requested data is performed among instantsand a long period of time. When it is data of the kind which it continues receiving over a long period of timereception of data will be succeedingly repeated within the user's B data receiver 5. This changes a situation according to the kind of data which the user B requested. The above is a series of data flow of the data transmission equipment by this invention.

[0017]The data format conversion of distributes data in the data distribution device 4next the data distribution device 4 is explained in detail. Firstthe data creation part 13 of the data donor's A data distribution device 4 is explainedreferring to drawing 2. It is accumulated in the data storing section 11 in the data distribution device 4 in the form where no multimedia data which a user needs is processed. The data storing section 11 told that the read request 10 of data came from the user B from the data management part 9 sends simultaneously the multimedia data 12 and the user's B Recipient information 30 which were requested to the IP packet preparing part 31 in the data creation part 13. In the user's B Recipient information 30it is an IP address required for IP packet transmission here. The data transmission equipment concerning this embodiment has assigned the IP address peculiar to all the contract users. While the user B has secured the IP address which the user B hasno users other than the

user B have.

[0018]The multimedia data 12 and IP address 30 addressed to user B which were sent from the data storing section 11 are sent to the IP packet preparing part 31. At the IP packet preparing part 31IP packet 32 is generated using IP address 30 which specifies the user B at the multimedia data 12 sent from the data storing section 11and its time. The size of this IP packet is prescribed by TCP/IP (Transmission Control Protocol/Internet Protocol)When the multimedia data which the user B requested exceeds that sizethis multimedia data is divided into two or more IP packetsand is transmitted to the following cryptopart 33.

[0019]The format of IP packet 32 used in the data transmission equipment concerning this embodiment is shown in drawing 4. Detailed explanation of each control bit in the IP header in an IP packet is omitted here. Howeverthe IP address which the user's B data receiver 5 has goes into the area of transmission destination IP address 61 in IP blanketand the IP address of the data donor's A data distribution device 4 goes into the area of transmitting agency IP address 60. The multimedia data 12 from the data storing section 11 in drawing 2 goes into the data division 53 in drawing 4.

[0020]IP packet 32 created by the IP packet preparing part 31 shown in drawing 2 is transmitted to the cryptopart 33. In the cryptopart 33it gets to know that Recipient is the user B by transmission destination IP address 61 in IP packet 32and the IP packet whole [32] is enciphered with the secret key which already becomes acquainted only between the data donor A and the user B at the time. As a cipher systemDES (Data EncryptionStandard) etc. are adoptedfor example. Since the IP address which the user B uses is included in the header of IP packet 32 hereit seems that it is not necessary to encipher with the secret key only for user Bbut. This is needed in order to prevent others' impersonating the user B using the user's B IP addressand using by stealth the data addressed to user B.

[0021]Howeverencryption does not encipher all the data to the user B and encryption may not be performed depending on the kind of data. When encryption is not performedIP packet 32 is directly transmitted to the MAC frame preparing part 36 from the IP packet preparing part 31. This embodiment describes the case where encryption is performed. Encryption is usually performed to a 64-bit plaintextand in not being a multiple whose data length of IP packet 32 which should be enciphered is 64 bitsit makes the whole IP packet into a 64-bit multiple by performing amends of data.e.the padding of invalid data.

[0022]The packet data 35 in which the IP packet 32 whole addressed to user B was enciphered are transmitted to the MAC frame preparing part 36. The format of MAC frame 37 is shown in drawing 5. In the MAC frame preparing part 36MAC header 119 as shown in drawing 5 is added to IP packet 35 addressed to user B enciphered by the cryptopart 33. Transmission destination IP address 54 in MAC header 119 is an IP address which the user B has. Herethe transmission destination IP address in enciphered IP packet 35 is the same as transmission destination IP address 54 of

MAC header 119. Thus MAC header 119 is attached because the data receiver 5 can know a transmission destination IP address only from MAC header 119 at the time of data receiving. That is since the user B cannot see a transmission destination address she cannot identify whether it is a packet addressed to itself only by the enciphered packet 35 until the data receiver 5 decodes the IP packet 35 enciphered whole. Therefore before the data receiver 5 decodes the IP packet which received in order for the IP packet to know that it is a thing addressed to itself transmission destination IP address 54 needs to be set to the header of a MAC frame. This transmission destination IP address 54 is directly passed to the MAC frame preparing part 36 from the IP packet preparing part 31.

[0023] PBL55 in MAC header 119 shown in drawing 5 is padding byte length and is the length of the invalid data covered on the occasion of encryption. This is needed in order that the user who received the enciphered IP packet may know regular data length. CP56 is a bit which identifies whether the multimedia data which a user needs or control data required for system management is contained in the IP packet. Usually CP56 of MAC frame 37 which should be received when a user requests shows that not control data but multimedia data is contained. EN57 in MAC header 119 is a control bit which shows whether the IP packet was enciphered by the cryptopart 33. As for a user decoding received MAC frame 37 determines whether lends and there is by this bit information. In the MAC frame preparing part 36 of drawing 2 it is added to IP packet (encryption is not carried out depending on the case) 35 as which the above control bit was enciphered.

[0024] MAC frame 37 generated by the MAC frame preparing part 36 of drawing 2 is transmitted to the CRC calculation part 38. In the CRC calculation part 38 a MAC frame 37 all byte's CRC (Cyclic Redundancy Checking: Cyclic Redundancy Check) which has been sent is calculated. In this embodiment CRC is 16 bits. Thus by calculating CRC the data receiver 5 can inspect whether the received MAC frame is correctly transmitted from the communications satellite 2. 16-bit CRC38a generated in the CRC calculation part 38 is added to the last of MAC frame 37 as shown in drawing 3 and drawing 5.

[0025] MAC frame 39 to which CRC38a was added is changed into the section which is transmitted to the section preparing part 40 and specified by MPEG 2. As shown in drawing 3 MAC frame 39 is added immediately after the section header (SecHd) 120. The format of the section header 120 is shown in drawing 6 (A). The format of the section header 120 shown by drawing 6 (A) is prescribed by MPEG 2 and has table id 100 the section sink indicator 101 the private indicator 102 reserved one 103 and the private section length 104. Here the data length of MAC frame 39 goes into the private section length 104.

[0026] The section 41 created by the section preparing part 40 shown in drawing 2 is transmitted to the transport packet preparing part 42. In the transport packet preparing part 42 the transmitted section format data is divided into the transport

packet 43 and it transmits to the following data transfer part 44.

[0027] The format of the packet header (TSHd) 121 of the transport packet 43 shown in drawing 3 is shown in drawing 6 (B). The header format of the transport packet 43 is prescribed by MPEG 2. As shown in drawing 6 (B), the packet header 121 of the transport packet 43 includes the sync byte 110, the transport error indicator 111, the payload unit start indicator 112, the transport priority 113, PID 114, the transport scramble control 115. It has the adaptation field control 116 and the Counter ***** 117. Since the size for one piece of the transport packet 43 is specified as 188 bytes, generally it is necessary to divide the one section 41 into two or more transport packets 43.

[0028] Since one section is not necessarily the integral multiple length of 184 bytes (number of bytes which subtracted 4 bytes of header length from 188 bytes), usually here when dividing the one section 41 into two or more transport packets 43, as shown in drawing 3, a data stopgap called stuffing is performed and the stuffing field 51 is formed. That is, when the one section 41 which is not 184 bytes of multiple is divided into two or more transport packets 43, all the bits 1 form the stuffing field 51 by which stuffing was carried out in the data area in which the last transport packet 43 remained.

[0029] Thus, after being transmitted to the data transfer part 44 and passing along data processing parts such as a multiplexer, the section 41 divided into two or more transport packets 43 is transmitted to the communications satellite 2 and is broadcast. The multimedia data for the broadcast user B will be received by the user's B data receiver 5. Reverse processing shown by drawing 2 will be performed by the data decomposition part 20, and the multimedia data requested eventually will arrive to the user B3.

Data receiver 5 [0030] fundamentally the concrete processing performed in the data decomposition part 20 of the data receiver 5 of the user B who shows drawing 2 can be set in the data creation part 13 of the data distribution device 4 and is a reverse algorithm of an algorithm. First, in the data receiving section 16 shown in drawing 1, the transport packet 43 shown in drawing 3 which received via the communications satellite 2 is combined, and the section 41 is generated. Next, the data receiving section 16 elongates the section 41, generates MAC frame 39, and outputs this to the data selection part 18. And in the data separation part 18, it is judged whether this transmission destination IP address 54 and the IP address of the data receiver 5 are in agreement based on transmission destination IP address 54 shown in drawing 5 contained in the Mac header 119 of MAC frame 39 shown in drawing 3. And the data separation part 18 sorts out the data concerned to a case and the bottom in agreement outputs it to the data decomposition part 20 as the data 19 which shows drawing 1 enciphered IP packet 35 which is shown in drawing 3 contained in this data. [0031] In the data decomposition part 20, after carrying out the double sign of enciphered IP packet 35 which is shown in drawing 3, inputted as the data 19 using the secret key which becomes acquainted only about between the data donors A

beforehand a data error inspection etc. are conducted. Here when there is a data error the data which performs processing to which data is returned or has the error concerned is canceled for example.

[0032] As explained above according to data transmission equipment concerning this embodiment and a method for the same use a TCP/IP communications protocol and. By providing a CRC bit in an IP packet even when digital data is transmitted to the data receiver 5 via the communications satellite 2 from the data distribution device 4 it controls effectively that a data transmission error occurs and quality digital data transmission can be realized. According to data transmission equipment concerning this embodiment and a method for the same data can be transmitted only to a specific user by transmitting an IP packet by a MAC frame method. According to data transmission equipment concerning this embodiment and a method for the same the data transmitted is enciphered and since only the data receiver 5 has a secret key which decrypts it the data concerned can prevent embezzling for others effectively.

[0033] This invention is not limited to the embodiment mentioned above. For example the data compression method of a MAC frame is not limited to MPEG 2 but other compression methods may be used for it. Internet Protocol is not limited to TCP/IP for example an OSI (Open Systems Interconnection) method may be used for it. although illustrated about the case where a secret key is used as an encryption method in this embodiment the same effect is acquired even if it uses a public key — things can be carried out.

[0034]

[Effect of the Invention] According to data transmission equipment of this invention and a method for the same even when transmitting data with radio system it controls effectively that a data transmission error occurs and quality digital data transmission can be realized. According to data transmission equipment of this invention and a method for the same data can be transmitted only not only to broadcast type data distribution but to the specific user of the singular number or plurality with radio system by adopting a MAC frame method. According to data transmission equipment of this invention and a method for the same the data concerned can prevent embezzling for others effectively by transmitting the enciphered data. The data transmission equipment which has the effect which was mentioned above is realizable by using the data distribution device and data receiver of this invention.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is a lineblock diagram of the data transmission equipment concerning the embodiment of this invention.

[Drawing 2] It is a lineblock diagram of the data distribution device shown in drawing 1.

[Drawing 3] It is a figure for explaining the processing in the data distribution device and data receiver which are shown in drawing 2.

[Drawing 4] It is a figure for explaining the format of an IP packet.

[Drawing 5] It is a figure for explaining the format of a MAC frame.

[Drawing 6] (A) is a figure for explaining the format of a section header (SecHd) and (B) is a figure for explaining the packet header (TSHd) of a transport packet.

[Description of Notations]

2 [— Data receiver] — A communications satellite 3 — ISDN 4 — A data distribution device 5 6 [— Data read demand] — A request 7 — A request reception part 9 — A data management part 10 11 — A data storing section 12 — Multimedia data 13 — Data creation part 14 — The data 16 which are transmitted with radio system — A data receiving section 18 — Data selection part 19 — The data which the user B can receive 20 — Data decomposition part 21 — Multimedia data 22 — A data execution part 31 — IP packet preparing part 33 — A cryptopart 26 — A MAC frame preparing part 38 — CRC calculation part 40 [— An IP packet 35 / — The IP packet 39 which were enciphered / — A MAC frame 120 / — A section header 121 / — A transport packet header 43 / — Transport packet] — A section preparing part 42 — A transport packet preparing part 44 — A data transfer part 32

特開平9-252320

(43) 公開日 平成 9 年 (1997) 9 月 22 日

(51) Int.Cl. ⁴	識別記号	序内整理番号	F I	技術表示箇所
H 0 4 L 12/56		9466-5K	H 0 4 L 11/20	1 0 2 A
G 0 6 F 13/00	3 5 1		G 0 6 F 13/00	3 5 1 L
H 0 4 B 7/00			H 0 4 B 7/00	
7/26			H 0 4 H 1/00	H
H 0 4 H 1/00			1/06	
審査請求 未請求 請求項の数 29 O L (全 10 頁) 最終頁に続く				

(21) 出願番号 特願平8-59745

(22) 出願日 平成 8 年 (1996) 3 月 15 日

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川 6 丁目 7 番 35 号

(72) 発明者 石井 眞

東京都品川区北品川 6 丁目 7 番 35 号 ソニ

ー株式会社内

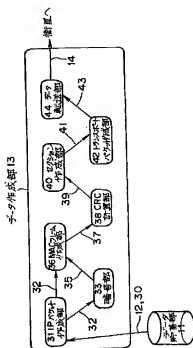
(74) 代理人 弁理士 佐藤 隆久

(54) 【発明の名称】 データ伝送装置およびその方法

(57) 【要約】

【課題】 高品質な無線方式のデジタルデータ伝送を、特定のユーザのみに行うことができるデータ伝送装置およびその方法を提供する。

【解決手段】 I P パケット作成部 3 4 で生成された I P パケット 3 2 を暗号部 3 3 で暗号化し、MAC フレーム作成部 3 6 において MAC ヘッダを付けて MAC フレーム 3 7 を生成する。次に、CRC 計算部 3 8 で CRC を形成し、これを MAC フレーム 3 7 に付加して MAC フレーム 3 9 を生成する。次に、セクション作成部 4 0 で MPEG 2 のセクション 4 1 を作成し、これをトランスポートパケット 4 3 に分割した後に、通信衛星を介して、サーバからクライアントに送信する。



【特許請求の範囲】

【請求項1】サーバとクライアント間のデータ伝送をネットワークを介して行うデータ伝送装置において、サーバとクライアント間で双方向のデータ伝送が可能な第1のデータ通信経路と、

前記サーバからクライアントにデータを無線方式で伝送可能で、前記第1のデータ通信経路に比べて伝送容量が大きな第2のデータ通信経路とを有し、

前記サーバは、複数のシステム相互間でネットワークを介してデジタルデータの送受信を行うためのインターネットプロトコルに基づいて、前記クライアントからの要求に応じたデータを、前記第2のデータ通信経路を介して前記クライアントに伝送するデータ伝送装置。

【請求項2】前記第1のデータ通信経路は、地上通信網を用いた経路であり、

前記第2のデータ通信経路は、通信衛星を用いた経路である請求項1に記載のデータ伝送装置。

【請求項3】前記インターネットプロトコルは、TCP/IPプロトコルである請求項1に記載のデータ伝送装置。

【請求項4】前記サーバは、伝送するデータをIPパケットに変換し、このIPパケットを、前記第2の通信経路を介して前記クライアントに伝送する請求項3に記載のデータ伝送装置。

【請求項5】前記サーバは、前記IPパケットからメディアアクセス制御(MAC)によってMACフレームを生成し、このMACフレームを、前記第2の通信経路を介して前記クライアントに伝送する請求項4に記載のデータ伝送装置。

【請求項6】前記サーバは、前記IPパケットを暗号化し、暗号化された1個の前記IPパケットについて、1個の前記MACフレームを生成する請求項5に記載のデータ伝送装置。

【請求項7】前記MACフレームのヘッダには、データを受け取るべきクライアントのIPアドレスと、データの暗号化の有無を示す制御ビットと、データが、クライアントからの要求に応じたメディアデータであるか、あるいはシステム運用のための制御データであるかを区別するための制御ビットと、データを暗号化するのに必要となるデータ長の正規化を行なった際の付加データ長を示すビットとが含まれる請求項5に記載のデータ伝送装置。

【請求項8】前記サーバは、要求を出した前記クライアントに配信するIPパケットを、当該サーバおよび当該クライアントのみが知る固有の暗号化アルゴリズムによって暗号化する手段と、メディアアクセス制御を用いて、前記暗号化されたIPパケットからMACフレームを作成する手段と、前記MACフレームをMPEG2で規定されたセクションに変換する手段と、

前記セクションを、MPEG2で規定されたトランスポートストリームに変換する手段と、

前記トランスポートストリームを前記第2の通信経路を介して前記クライアントに伝送する手段とを有する請求項4に記載のデータ伝送装置。

【請求項9】前記サーバおよび前記クライアントは、CRC方式によって、前記MACフレームの全データバイトを検査する手段をさらに有する請求項5に記載のデータ伝送装置。

【請求項10】前記サーバは、MACフレームについてのCRC検査ビットを、MACフレームの最後に付加する手段をさらに有する請求項5に記載のデータ伝送装置。

【請求項11】前記サーバは、MACフレームについてのCRC検査ビットを、MACフレームの最後に付加する手段をさらに有する請求項9に記載のデータ伝送装置。

【請求項12】クライアントとの間のデータ伝送をネットワークを介して行うデータ配信装置において、当該データ配信装置とクライアント間で双方向のデータ伝送が可能な第1のデータ通信経路に接続された第1のインターフェースと、当該データ配信装置からクライアントにデータを無線方式で伝送可能で、前記第1のデータ通信経路に比べて伝送容量が大きな第2のデータ通信経路に接続された第2のインターフェースとを有し、

複数のシステム相互間でネットワークを介してデジタルデータの送受信を行うためのインターネットプロトコルに基づいて、前記クライアントからの要求に応じたデータを、前記第2のデータ通信経路を介して前記クライアントに伝送するデータ配信装置。

【請求項13】送信するデータをIPパケットに変換し、このIPパケットを、前記第2の通信経路を介して前記クライアントに伝送する請求項12に記載のデータ配信装置。

【請求項14】前記IPパケットを暗号化し、暗号化された1個の前記IPパケットについて、1個の前記メディアアクセス制御によるMACフレームを生成し、当該MACフレームを伝送する請求項13に記載のデータ配信装置。

【請求項15】要求を出した前記クライアントに配信するIPパケットを、当該データ配信装置および当該クライアントのみが知る固有の暗号化アルゴリズムによって暗号化する手段と、メディアアクセス制御を用いて、前記暗号化されたIPパケットからMACフレームを作成する手段と、前記MACフレームをMPEG2で規定されたセクションに変換する手段と、前記セクションを、MPEG2で規定されたトランスポートストリームに変換する手段と、

前記トランスポートストリームを前記第2の通信経路を介して前記クライアントに伝送する手段とを有する請求項14に記載のデータ配信装置。

【請求項16】サーバとの間のデータ伝送をネットワークを介して行うデータ受信装置において、

前記サーバと当該データ受信装置間で双方向のデータ伝送が可能な第1のデータ通信経路に接続された第1のインターフェースと、

前記サーバから当該データ受信装置にデータを無線方式で伝送可能で、前記第1のデータ通信経路に比べて伝送容量が大きな第2のデータ通信経路に接続された第2のインターフェースとを有し、

複数のシステム相互間でネットワークを介してデジタルデータの送受信を行うためのインターネットプロトコルに基づいて、前記サーバからのデータを、前記第2のデータ通信経路を介して受信するデータ受信装置。

【請求項17】前記受信するデータは、IPパケット形式のデータである請求項16に記載のデータ受信装置。

【請求項18】前記受信するデータに含まれるメディアアクセス制御によるMACフレームのヘッダに基づいて、必要なIPパケットを選択的に取り込む請求項17に記載のデータ受信装置。

【請求項19】サーバとクライアント間で双方向のデータ伝送が可能な第1のデータ通信経路と、前記サーバからクライアントにデータを無線方式で伝送可能で、前記第1のデータ通信経路に比べて伝送容量が大きな第2のデータ通信経路とを有するネットワークを介してサーバとクライアント間のデータ伝送を行うデータ伝送方法であって、

前記サーバは、複数のシステム相互間でネットワークを介してデジタルデータの送受信を行うためのインターネットプロトコルに基づいて、前記クライアントからの要求に応じたデータを、前記第2のデータ通信経路を介して前記クライアントに伝送するデータ伝送方法。

【請求項20】前記第1のデータ通信経路は、地上通信網を用いた経路であり、

前記第2のデータ通信経路は、通信衛星を用いた経路である請求項19に記載のデータ伝送方法。

【請求項21】前記インターネットプロトコルは、TCP/IPプロトコルである請求項19に記載のデータ伝送方法。

【請求項22】前記サーバは、伝送するデータをIPパケットに変換し、このIPパケットを、前記第2の通信経路を介して前記クライアントに伝送する請求項21に記載のデータ伝送方法。

【請求項23】前記サーバは、前記IPパケットからメディアアクセス制御(MAC)によってMACフレームを生成し、このMACフレームを、前記第2の通信経路を介して前記クライアントに伝送する請求項22に記載のデータ伝送方法。

【請求項24】前記サーバは、前記IPパケットを暗号化し、暗号化された1個の前記IPパケットについて、1個の前記MACフレームを生成する請求項23に記載のデータ伝送方法。

【請求項25】前記MACフレームのヘッダには、データを受け取るべきクライアントのIPアドレスと、データの暗号化の有無を示す制御ビットと、データが、クライアントからの要求に応じたメディアデータであるか、あるいはシステム運用のための制御データであるかを区別するための制御ビットと、データを暗号化するのに必要となるデータ長の正規化を行なった際の付加データ長を示すビットとが含まれる請求項23に記載のデータ伝送方法。

【請求項26】前記サーバは、要求を出した前記クライアントに配信するIPパケットを、当該サーバおよび当該クライアントのみが知る固有の暗号化アルゴリズムによって暗号化する手段と、メディアアクセス制御を用いて、前記暗号化されたIPパケットからMACフレームを作成する手段と、前記MACフレームをMPEG2で規定されたセクションに変換する手段と、前記セクションを、MPEG2で規定されたトランスポートストリームに変換する手段と、前記トランスポートストリームを前記第2の通信経路を介して前記クライアントに伝送する手段とを有する請求項22に記載のデータ伝送方法。

【請求項27】前記サーバおよび前記クライアントは、CRC方式によって、前記MACフレームの全データバイトを検査する手段をさらに有する請求項23に記載のデータ伝送方法。

【請求項28】前記サーバは、MACフレームについてのCRC検査ビットを、MACフレームの最後に付加する手段をさらに有する請求項23に記載のデータ伝送方法。

【請求項29】前記サーバは、MACフレームについてのCRC検査ビットを、MACフレームの最後に付加する手段をさらに有する請求項27に記載のデータ伝送方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えば、通信衛星を用いて、マルチメディアデータ配信サービスを行うためのデータ伝送装置およびその方法に関する。

【0002】

【従来の技術】従来、テレビ放送などの通信衛星を用いたデータ配信サービスでは、データの流れは、データ配信者からユーザへの一方のみであった。近年、通信衛星を用いたデジタルデータの伝送が可能になったことで、テレビや映画などのアナログ映像・音声データのみならず、コンピュータなどで利用されるテキストやデジ

タル映像・音声データについても、通信衛星を用いて伝送されるようになった。ここで、テレビ放送などの通信衛星を使った従来のデータ配信サービスは、データ配信者が配信したデータを同時に多数のユーザが受信して使用する形態である。これに対して、コンピュータなどで使用されるデジタルデータを、通信衛星を介して配信する場合には、データ配信者から単数または複数の特定のユーザにデータを配信する機能が求められる。

【0003】

【発明が解決しようとする課題】しかしながら、通信衛星を用いた従来の伝送方式では、アナログデータの配信であることや、データ配信はデータ配信者からユーザへの一方のみであることから、伝送上のエラーをチェック機能は備えておらず、データ伝送の信頼性が低いという問題がある。デジタルデータの配信では、伝送によってデータに1ビットでも誤りが生じると、受信したデータは無意味なものになってしまう。このようなデジタルのコンピュータデータを無線方式で高品質に配信するためには、データ配信者からユーザへの一方のデータ配信だけでなく、ユーザからデータ配信者への通信路を確保する必要があるが、従来の伝送方式では、このような機能を備えていない。

【0004】また、従来のデータ配信者から多ユーザへの同時通信又は放送システムでは、全ユーザは常に同じ情報を受信して使用または閲覧しており、システムユーザ個人の識別情報がないため、データ配信者から特定ユーザのみへのデータの配信ができないという問題がある。

【0005】本発明は上述した従来技術の問題点に鑑みてなされ、伝送上のエラーを発生させることなく、デジタルデータを無線方式で伝送できるデータ伝送装置およびその方法を提供することを目的とする。また、本発明は、特定のクライアントのみに、デジタルデータを無線方式で伝送できるデータ伝送装置およびその方法を提供することを目的とする。

【0006】

【課題を解決するための手段】上述した目的を達成するために、本発明のデータ伝送装置は、サーバとクライアント間で双方向のデータ伝送が可能な第1のデータ通信経路と、前記サーバからクライアントにデータを無線方式で伝送可能で、前記第1のデータ通信経路に比べて伝送容量が大きな第2のデータ通信経路とを有し、前記サーバは、複数のシステム相互間でネットワークを介してデジタルデータの送受信を行うためのインターネットプロトコルに基づいて、前記クライアントからの要求に応じたデータを、前記第2のデータ通信経路を介して前記クライアントに伝送する。

【0007】また、本発明のデータ伝送方法は、サーバとクライアント間で双方向のデータ伝送が可能な第1のデータ通信経路と、前記サーバからクライアントにデー

タを無線方式で伝送可能で、前記第1のデータ通信経路に比べて伝送容量が大きな第2のデータ通信経路とを有するネットワークを介してサーバとクライアント間のデータ伝送を行うデータ伝送方法であって、前記サーバは、複数のシステム相互間でネットワークを介してデジタルデータの送受信を行うためのインターネットプロトコルに基づいて、前記クライアントからの要求に応じたデータを、前記第2のデータ通信経路を介して前記クライアントに伝送する。

【0008】本発明のデータ伝送装置およびその方法では、例えばクライアントが第1のデータ通信経路を介して所定のリクエストをサーバに行くと、サーバにおいて、当該リクエストに応じたデータをインターネットプロトコルに基づいて変換し、この変換したデジタルデータを第2のデータ通信経路を介してクライアントに伝送する。

【0009】本発明によるデータ伝送装置およびその方法によれば、サーバからクライアントに大容量なデジタルデータを高品質に伝送が可能となり、さらに、サーバから特定のユーザにのみデジタルデータの転送が可能となる。

【0010】

【発明の実施の形態】本発明の実施形態に係るデータ伝送装置（情報提供システム）およびその方法について説明する。図1に、マルチメディアのデジタルデータ（映像、音声、テキスト等）を配信するデータサービスを実現するためのデータ伝送装置の概略を示す。図1に示すデータ伝送装置では、データ提供者Aはサーバとしてのデータ配信装置4を所有し、ユーザBはクライアントとしてのデータ受信装置5を所有している。データ配信装置4およびデータ受信装置5は、双方向の通信が可能なISDN3を介して相互に通信が可能である。また、データ配信装置4から、データ受信装置5へは、通信衛星2を介して、無線方式で大容量の通信が可能である。

【0011】図1に示すデータ伝送装置におけるデータの流れを説明する。ユーザ提供者AとユーザBが、マルチメディアデータの配送の契約を予め結んでいるものとする。この際、ユーザBのデータ受信装置5にはデータ提供者Aのデータ配信装置4からデータを受信できる機能が備わっているとす。さらに、データ提供者Aは、予めユーザBとの契約が結ばれていることを知っている。

【0012】先ず、ユーザBは、例えば、地上通信網としてのISDN3を介して、データ提供者Aが提供する所定のサービスを受けた旨のリクエスト6をデータ提供者Aに送る。このリクエスト6を送る方法は、特に限定されず、データの種類やユーザとの契約状況によって決められ、例えば郵便などでもよい。また、リクエスト6を送らずに、予め契約に従って、データ提供者Aがサー

ビスを提供してもよい。

【0013】データ配信装置4に送られたユーザBからのリクエスト6は、データリクエスト受付部7で受け取られ、データ管理部9に送られる。データ管理部9は、ユーザBの契約情報やリクエスト6が意味のあるものか否かのチェックを行ない、問題が無ければ、データ貯蓄部11にデータの読み出し要求10を行なう。データ貯蓄部11は、データ読み出し要求10に応じた、例えばマルチメディアデータ12をデータ作成部13へ送る。データ作成部13では、データ貯蓄部11からのマルチメディアデータ12に対してIPパケット化、予めユーザBに対して固有に決められた暗号化、MAC(Media Access Control) フレーム化、MPEG(Moving Picture Experts Group) 2のトランスポート化などのデータのフォーマット変換が行なわれる。このデータフォーマット変換についての後述する。

【0014】データ貯蓄部11からのマルチメディアデータ12は、データ作成部13によって作成又はフォーマット変換された後、データ14として通信衛星2に送られる。通信衛星2を介して送られたデータ14は、ユーザBのデータ受信装置5に限らず、データを受信できる状況にある全てのユーザが受信することが可能である。データ受信装置5は、通信衛星2からの全データを受信し、その中から、自分が出したリクエスト6に応じたデータを選別して受け取る。

【0015】すなわち、データ受信装置5は、リクエスト6に応じた送信されたデータを含む多数のデータ14をデータ受信部16で受信する。データ受信装置5は、その中から、自分宛のデータ、自分が受け取るべきデータ、自分が受け取るとことができるデータ(これは契約にもよる)を選別する。この選別は、データ受信装置5のデータ選択部18において行われる。尚、予めユーザBとデータ提供者Aとの契約によって、ユーザBが持つデータ受信装置5は決定されている。従って、ユーザBが持つデータ受信装置5を用いて、他のユーザ宛の特有のデータは選別することができない。

【0016】データ選択部18において、ユーザBが受け取ることが可能なデータ19は全てデータ分解部20に送られる。データ分解部20に送られたユーザB宛のデータは、分解もしくは復号されてマルチメディアデータ21となり、データ実行部22へ送られる。これによってユーザBのみが、ユーザBがリクエストしたユーザB宛のデータを受信することができ、このデータサービスが完了する。尚、リクエストしたデータの受信は、一瞬のうち行われる場合と、長期間にわたって続けられる場合がある。長期間にわたって受信続ける種類のデータであった場合には、ユーザBのデータ受信装置5内で、データの受信が引き続き繰り返されることになる。これは、ユーザBがリクエストしたデータの種類によって状況が変わる。以上が、本発明によるデータ伝送装置の一

連のデータの流れである。

【0017】データ配信装置4

次に、データ配信装置4における、配信データのデータフォーマット変換について詳細に説明する。まず、図2を参照しながら、データ提供者Aのデータ配信装置4のデータ作成部13について説明する。データ配信装置4内のデータ貯蓄部11には、ユーザが必要とするマルチメディアデータが何も加工されていないかたちで蓄積されている。データ管理部9から、データの読み出し要求10がユーザBから来たことを知らされたデータ貯蓄部11は、リクエストされたマルチメディアデータ12およびユーザBのあて先情報30を同時にデータ作成部13内のIPパケット作成部31に送る。ここでユーザBのあて先情報30とは、IPパケット送信に必要なIPアドレスである。本実施形態に係るデータ伝送装置は、すべての契約ユーザに固有のIPアドレスを割り振っている。ユーザBが持つIPアドレスは、ユーザBが確保している間は、ユーザB以外のユーザは持たない。

【0018】データ貯蓄部11から送られたユーザB宛のマルチメディアデータ12およびIPアドレス30はIPパケット作成部31に送られる。IPパケット作成部31では、データ貯蓄部11から送られてきたマルチメディアデータ12とその時点でユーザBを特定するIPアドレス30を用いて、IPパケット32を生成する。このIPパケットの大きさはTCP/IP(Transmission Control Protocol/Internet Protocol)で規定され、ユーザBがリクエストしたマルチメディアデータは複数のIPパケットに分割されて次の暗号部33に転送される。

【0019】本実施形態に係るデータ伝送装置において使用されるIPパケット32のフォーマットを図4に示す。IPパケット内のIPヘッダ内の各制約ビットの詳しい説明はここでは省略する。ただし、IPケット内の送信先IPアドレス61のエリアにはユーザBのデータ受信装置5が持つIPアドレスが入り、送信元IPアドレス60のエリアにはデータ提供者Aのデータ配信装置4のIPアドレスが入る。さらに、図4内のデータ部53には図2におけるデータ貯蓄部11からのマルチメディアデータ12が入る。

【0020】図2に示すIPパケット作成部31で作成されたIPパケット32は、暗号部33に転送される。暗号部33では、IPパケット32内の送信先IPアドレス61によって、あて先がユーザBであることを知り、その時点で既にデータ提供者AとユーザBとの間のみで知りあう秘密鍵によってIPパケット全体32を暗号化する。暗号化方式としては、例えばDES(Data Encryption Standard)などが採用される。ここで、IPパケット32のヘッダにはユーザBのみが利用できるIPアドレスが含まれるのでユーザB専用の秘密鍵で暗号化する

必要はないように思われるが、これは他人がユーザBのIPアドレスを用いてユーザBに成り済ましてユーザB宛のデータを盗用することを防ぐために必要となる。

【0021】ただし、暗号化はユーザBに対する全てのデータを暗号化するわけではなく、データの種類によっては暗号化が行なわれないこともある。暗号化が行われない場合には、IPパケット作成部31からMACフレーム作成部36に直接IPパケット32が転送される。本実施形態では、暗号化が行なわれる場合について述べる。暗号化は通常64ビットの平文に対して行なわれ、暗号化すべきIPパケット32のデータ長が64ビットの倍数でない場合には、データの埋め合わせ、すなわち、無効データのパディングを行うことでIPパケット全体を64ビットの倍数にする。

【0022】ユーザB宛のIPパケット32全体が暗号化されたパケットデータ35は、MACフレーム作成部36に転送される。MACフレーム37のフォーマットを図5に示す。MACフレーム作成部36では、暗号部33によって暗号化されたユーザB宛のIPパケット35に対して、図5に示す通りのMACヘッダ119を付加する。MACヘッダ119内の送信先IPアドレス54はユーザBが持つIPアドレスである。ここで、MACヘッダ119の送信先IPアドレス54と、暗号化されたIPパケット35内の送信先IPアドレスとは同じである。このように、MACヘッダ119を付けるのは、データ受信装置5はデータ受信時において、MACヘッダ119からのみ送信先IPアドレスを知ることができするためである。すなわち、データ受信装置5は、暗号化されたIPパケット35全体を復号するまでユーザBは送信先IPアドレスを見ることができないため、暗号化されたパケット35のみでは、自分宛のパケットかどうかを識別できない。従って、データ受信装置5が、受信したIPパケットを復号する前に、そのIPパケットが自分宛のものであることを知るために、MACフレームのヘッダに送信先IPアドレス54がセットされる必要がある。この送信先IPアドレス54は、IPパケット作成部31からMACフレーム作成部36に直接渡される。

【0023】また、図5に示すMACヘッダ119内のPBL55はパディングバイト長であり、暗号化の際に埋め合わせされた無効なデータの長さである。これは、暗号化されたIPパケットを受信したユーザが正確なデータ長を知るために必要となる。また、CP56は、IPパケットに、ユーザが必要なマルチメディアデータシステム運用に必要な制御データが入っているかを識別するビットである。通常、ユーザがリクエストした際に受け取るべきMACフレーム37のCP56は、制御データでなくマルチメディアデータが入っていることを示している。MACヘッダ119内のEN57は、IPパケットが暗号部33によって暗号化されたかどうか

を示す制御ビットである。このビット情報によってユーザは受信したMACフレーム37を復号をするかしないか決定する。図2のMACフレーム作成部36では、以上の制御ビットが暗号化された（場合によっては暗号化はされない）IPパケット35に付加される。

【0024】図2のMACフレーム作成部36で生成されたMACフレーム37は、CRC計算部38に転送される。CRC計算部38では、送られてきたMACフレーム37全バイトのCRC（Cyclic Redundancy Check：巡回冗長検査）の計算を行う。本実施形態では、CRCは16ビットである。このようにCRCの計算を行うことで、データ受信装置5は、受信したMACフレームが正しく通信衛星2から伝送されているかを確認することができる。CRC計算部38において生成された16ビットのCRC38aは、図3、図5に示すように、MACフレーム37の最後に付加される。

【0025】CRC38aが付加されたMACフレーム39は、セクション作成部40に転送されてMPEG2で規定されるセクションに変換される。図3に示すように、MACフレーム39は、セクションヘッダ（Section Header）120の直後に付加される。セクションヘッダ120のフォーマットを図6（A）に示す。図6（A）で示したセクションヘッダ120のフォーマットは、MPEG2によって規定され、テーブルid100、セクションシンクインディケータ101、プライベートインディケータ102、リザーブ103、プライベートセクションレングス104を有する。ここで、プライベートセクションレングス104には、MACフレーム39のデータ長が入る。

【0026】図2に示すセクション作成部40で作成されたセクション41は、トランスポートパケット作成部42に転送される。トランスポートパケット作成部42では、転送されたセクションフォーマットデータをトランスポートパケット43に分割して次のデータ転送部44に転送する。

【0027】図3に示すトランスポートパケット43のバケットヘッダ（TSHd）121のフォーマットを図6（B）に示す。トランスポートパケット43のバケットヘッダ121は、シンクバイト110、トランスポートエラーインディケータ111、ペイロードユニットスタートインディケータ112、トランスポートプライオリティ113、PID114、トランスポートスクランブルコントロール115、アダプティオンフィールドコントロール116およびコンディニティカウンタ117を有する。トランスポートパケット43の1個分の大きさは188バイトと規定されているので、一般的に、一つのセクション41を複数のトランスポートパケット43に分割する必要がある。

る。

【0028】ここで、通常、一つのセクションは184バイト(188バイトからヘッダ長の4バイトを引いたバイト数)の整数倍長とは限らないので、一つのセクション41を複数のトランスポートバケット43に分割する際に、図3に示すように、スタッフィングと呼ばれるデータ穴埋めを行い、スタッフィング領域51を形成する。すなわち、184バイトの倍数でない一つのセクション41を複数のトランスポートバケット43に分割した場合、最後のトランスポートバケット43の余ったデータエリアに、全てのビット1がスタッフィングされたスタッフィング領域51を形成する。

【0029】このように複数のトランスポートバケット43に分割されたセクション41は、データ転送部44に転送され、マルチプレクサなどのデータ処理部を通った後、通信衛星2に伝送され、ブロードキャストされる。ブロードキャストされたユーザBのためのマルチメディアデータは、ユーザBのデータ受信装置5によって受信され、図2に示した逆の処理がデータ分解部2によって行われ、最終的にリクエストされたマルチメディアデータはユーザBの手元に届くこととなる。

データ受信装置5

【0030】図2に示すユーザBのデータ受信装置5のデータ分解部2において行なわれる具体的な処理は、基本的には、データ配信装置4のデータ作成部13におけるアルゴリズムの逆アルゴリズムである。先ず、図1に示すデータ受信部16において、通信衛星2を介して受信した図3に示すトランスポートバケット43を結合してセクション41を生成する。次に、データ受信部16は、セクション41を伸長して、MACフレーム39を生成し、これをデータ選択部18に出力する。そして、データ選択部18において、図3に示すMACフレーム39のマックヘッダ119に含まれる図5に示す送信先IPアドレス54に基づいて、この送信先IPアドレス54とデータ受信装置5のIPアドレスとが一致するかを判断する。そして、データ選択部18は、一致する場合に、当該データを選択し、このデータに含まれる図3に示す暗号化されたIPバケット35を図1に示すデータ19としてデータ分解部20に出力する。

【0031】データ分解部20では、データ19として入力した図3に示す暗号化されたIPバケット35を、予めデータ提供者Aとの間のみを知らう秘密鍵を用いて復号した後、データ誤り検査などを行う。ここで、例えば、データ誤りがある場合には、データを復号させる処理を行うか、あるいは、当該誤りのあるデータを破棄する。

【0032】以上説明したように、本実施形態に係わるデータ伝送装置およびその方法によれば、TCP/IP通信プロトコルを用いと共に、IPバケットにCRCビットを設けることで、データ配信装置4から通信衛星

2を介してデータ受信装置5にデジタルデータを伝送した場合でも、データ伝送エラーが発生することを効果的に抑制し、高品質なデジタルデータ転送を実現できる。また、本実施形態に係わるデータ伝送装置およびその方法によれば、IPバケットをMACフレーム方式で伝送することで、特定のユーザのみにデータを伝送することができる。また、本実施形態に係わるデータ伝送装置およびその方法によれば、伝送されるデータは暗号化されており、データ受信装置5のみが、それを復号化する秘密鍵を持っていることから、当該データが他人に盗用されることを効果的に防止できる。

【0033】本発明は上述した実施形態には限定されない。例えば、MACフレームのデータ圧縮方法は、MP EG2には限定されず、他の圧縮方法を用いてもよい。また、インターネットプロトコルは、TCP/IPには限定されず、例えばOSI (Open Systems Interconnection)方式を用いてもよい。さらに、本実施形態では、暗号化方法として、秘密鍵を用いる場合について例示したが、公開鍵を用いても同様な効果を得ることできる。

【0034】

【発明の効果】本発明のデータ伝送装置およびその方法によれば、無線方式でデータを送信する場合でも、データ伝送エラーが発生することを効果的に抑制し、高品質なデジタルデータ転送を実現できる。また、本発明のデータ伝送装置およびその方法によれば、MACフレーム方式を採用することで、ブロードキャスト型のデータ配信のみならず、単数または複数の特定のユーザのみにデータを無線方式で伝送することができる。また、本発明のデータ伝送装置およびその方法によれば、暗号化されたデータを伝送することで、当該データが他人に盗用されることを効果的に防止できる。また、本発明のデータ配信装置およびデータ受信装置を用いることで、上述のような効果をも有するデータ伝送装置を実現できる。

【図面の簡単な説明】

【図1】本発明の実施形態に係わるデータ伝送装置の構成図である。

【図2】図1に示すデータ配信装置の構成図である。

【図3】図2に示すデータ配信装置およびデータ受信装置における処理を説明するための図である。

【図4】IPバケットのフォーマットを説明するための図である。

【図5】MACフレームのフォーマットを説明するための図である。

【図6】(A)はセクションヘッダ(Sechd)のフォーマットを説明するための図であり、(B)はトランスポートバケットのバケットヘッダ(TShd)を説明するための図である。

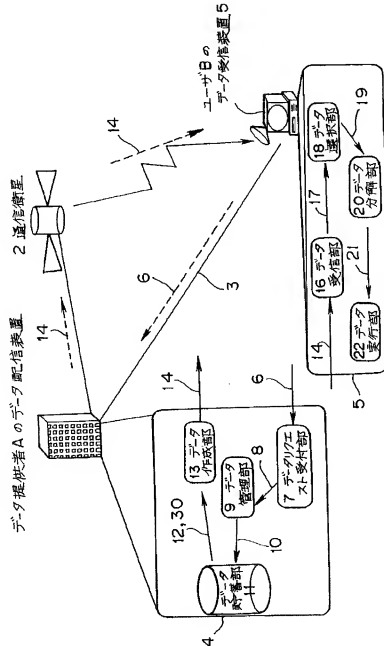
【符号の説明】

2…通信衛星、3…IP SDN、4…データ配信装置、5…データ受信装置、6…リクエスト、7…リクエスト受

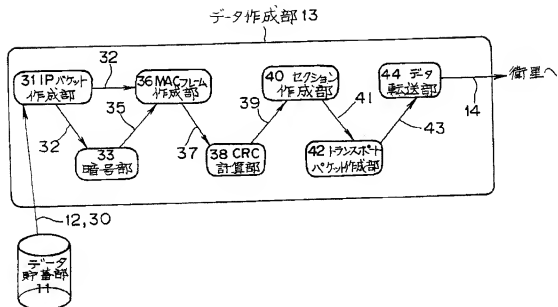
付部、9…データ管理部、10…データ読み出し要求、
11…データ貯蓄部、12…マルチメディアデータ、1
3…データ作成部、14…無線方式で伝送するデータ、
16…データ受信部、18…データ選択部、19…ユー
ザBが受け取ることができるデータ、20…データ分解
部、21…マルチメディアデータ、22…データ実行
部、31…IPパケット作成部、33…暗号部、26…

MACフレーム作成部、38…CRC計算部、40…セ
クション作成部、42…トランスポートパケット作
成部、44…データ転送部、32…IPパケット、35…
暗号化されたIPパケット、39…MACフレーム、1
20…セクションヘッダ、121…トランスポートパ
ケットヘッダ、43…トランスポートパケット

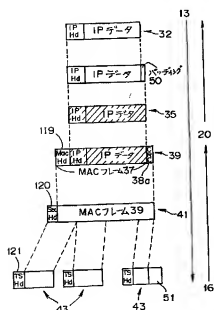
【図1】



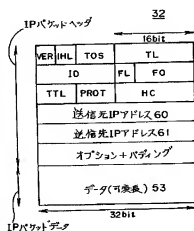
【図2】



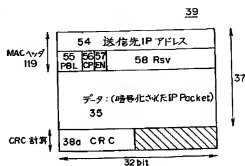
【図3】



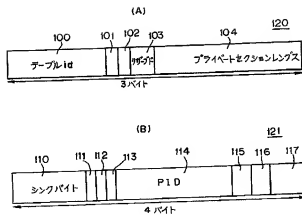
【図4】



【図5】



【図6】



フロントページの続き

(51) Int. Cl.⁶

H 0 4 H 1/08

識別記号

庁内整理番号

F I

H 0 4 B 7/26

技術表示箇所

M